ISSN 2582-0311 (Print)
ISSN 2582-0303 (Online)

Volume 3
Issue I

August 2021

VIPS STUDENT LAW REVIEW

VIVEKANANDA INSTITUTE OF PROFESSIONAL STUDIES
ISO 9001:2015 Certified Institution
(Affiliated to GGSIP University & Approved by BCI & AICTE)
The Institute is NAAC Accredited 'A' Grade, recognized by UGC under section 2(f)
& NBA Accredited for MCA Programme

Volume 3, Issue I August, 2021 ISSN 2582-0311 (Print)
ISSN 2582-0303 (Online)

TABLE OF CONTENTS

S. No. Title of the Paper/ Author **Page No.**

1. An Era Comes To An End: Soli- A Great Lawyer And A True Friend
V. Sudhish Pai 1

2. Pre-empting A rise in Human Trafficking: A Deadly Side Effect of the COVID-19 Pandemic
Shivani Chawla 7

3. Efficacy of Victim Impact Statement in Indian Criminal Justice System in the Light of International Experiences
Samriti Verma and Anuj Kumar Tiwari 23

4. Psychological Autopsy
Lovleen Sharma 36

5. Constitutional Courts and Judicial Independence: Conceptualising Judicial Dissent in South Asian Perspective
Neha Tripathi and Anubhav Kumar 44

6. Work From Home and The Need for Right to Disconnect: Aftermath of the COVID-19 Pandemic
Shivya Juneja and Divyanshu Priyadarshi 61

STUDENTS

7. Liability Dimension of The Chamoli Disaster in Uttarakhand Under the Legal Framework
Sarthak Aryan and Jayanta Boruah 73

8. The Role of Nyaya Panchayat in Delivery of Rural Justice in India: A Critical Analysis
Namrata Chakraborty and Himanshu Anand 83

9. Inadequate Environmental Laws and increasing Pollution in Space
Deepansh Tripathi 94

10. An Unvaccinated World: The Intellectual Property Rights Conundrum
Nishita Arora and Hiba Nasir 105

11. Regulating the Unregulated Video-On-Demand Platforms in India
Ravi Singh Chhikara and Abhinav Arora 114

12. Utility Model System: Need of the Hour for Small Innovators
Girish Ahuja and Aparna Singh 130

13. CSR and Ghost Beneficiaries: The New Age Fraud Mechanism
Kushal Tekriwal 145

14. The 'Unpolished' Code Barricading Cross- Border Insolvency In India.
Prateek Khandelwal and Poojal Agarwal 154

15. Evaluation of Multiculturalism and Gender Equality in Family Laws of India from Uniform Civil Code Perspective
Tejash Bhandari 167

16. Protest: Defending the Right to Protest in the Digital Age
Neha Maria Antony 177

17. Is Gambling Safe Haven for Taxation? Understanding the Applicability of GST Laws in the Gambling Industry
Sagnik Sarkar 188

18. Applicability of the POSH Act to the Virtual Workplace: Assessing the New Normal
Gunjan Garg 202

19. Cyber Defense Policy Framework and Response Mechanisms towards the Cyber Threats and Emerging Cyber Warfares
Kshitij Dahiya and Vasu Manchanda 216

CASE COMMENTS

20. To Report or Not To Report: Zooming in the Case of Chief Election Commissioner of India v/s M.R. Vijayabhaskar & Ors.
Prerna Dhingra 228

21. An Approach Towards Balancing Fundamental Rights: Amit Sahni v/s Commissioner of Police
Sarthak Bhardwaj 237

LEGISLATIVE REVIEW

22. The Hindu Marriage Act of Pakistan: A Spearhead of Social Change
Kavish Arora 247

23. Critical Analysis of Civil Liability for Nuclear Damage Act, 2010
Ayush Garg and Mridul Pateriya 256

BOOK REVIEW

24. Rashmi Salpekar and Gauri Gupta, *Moot Problems*
(Vivekananda Institute of Professional Studies, 2021)
Shweta Shukla 269

Cyber Defense Policy Framework and Response Mechanisms Towards the Cyber Threats and Emerging Cyber Warfare

VIPS Student Law Review
August 2021, Vol. 3, Issue 1, 216-227
ISSN 2582-0311 (Print)
ISSN 2582-0303 (Online)
© Vivekananda Institute of Professional Studies
https://vslls.vips.edu/vslr/

Kshitij Dahiya*
Vasu Manchanda**

Abstract

The domestic infrastructure contradicts the defensive structure of the global agencies, which has resulted in the awakening of the notion of cyber security and thus enhanced surveillance over the web world. A comprehensive and situational approach must emerge from social, political and legal reforms, which necessitates cyber defense mechanism and intelligence capabilities for monitoring the state and non-state factors at the same time towards cyber threats, cyber violence and cyber-attacks. The challenges posed are increasingly complex, and the need of the hour is a multi-disciplinary approach by various stakeholders to the responses and solutions. This paper argues that facing global cyber threats with local resources is not enough. Countries need to do more internally and internationally than just prepare antivirus, firewall or data encryption provisions to prevent cyber-crimes. Capital investment needs to be made in formulating cyber defense strategies and framework, strengthening international institutions and regulators and there needs to be a crisis protocol in place to provide cushioning to global financial systems.

Introduction

Cyber-attacks have the potential of leaving the world in a more disintegrated state than the novel-coronavirus pandemic (COVID-19). According to a study conducted by Specops

* Student, 2nd year, Faculty of Law, University of Delhi, Delhi, India.
** Student, 3rd year, Faculty of Law, University of Delhi, Delhi, India.

Software, cyber-attacks are expected to cost the global economy $6 trillion dollars per year by 2021.[1] Such attacks have surged by 260% during the COVID-19 pandemic with phishing emails being the most popular attack vector.[2]

This makes it all the more imperative for countries to be proactive in preparing for the potential cyber-attacks collectively. Facing global cyber threats with local resources is not enough. Multilateralism is the need of the hour. Countries need to do more internally and internationally than just prepare antivirus, firewalls, and enable data localisation, pseudonymization and data encryption provisions to avert cyber wrongdoings. Capital investment needs to be made in formulating cyber defense and cyber offense strategies and frameworks, strengthening international institutions and regulators. There needs to be a crisis protocol in place to provide cushioning to global financial systems.

It is noteworthy that contemporary developments in cyber space have exposed to a variety of threats to national security, privacy, data protection and retention and others which is further necessitating rigorous measures vis-à-vis the development of cyber infrastructure. The information revolution has transformed lives across boundaries with increased dependency over the web framework and network which brings forth cyber challenges in the form of security, warfares, intelligence, threats and others concerns. The continuous evolution of threats in various degrees is mandating the political as well as policy corridors to address the looming concerns with immediate and intense attention thereby addressing the vulnerabilities and challenges.

Cyber Defense

Cyber defense[3] by the very virtue means pre-defensive measures to safeguard data and organisational assets from unauthorised cyber threats and attacks. It involves a wide array of activities to enable an organisation to protect itself against attack. It includes attack detection capability to spot when hackers/attackers are targeting the firm; response and reaction capabilities to repel them; and cyber deterrents to reduce the organization's appeal to the attacker.

1 Correspondent, *India third among countries targeted by cyber attackers*, Campaign India (Jul. 19, 2020), https://www.campaignindia.in/article/india-third-among-countries-targeted-by-cyber-attackers-report/462313.

2 Abhijit Ahaskar, *Coronavirus related cyberattacks surge by 260% during lockdown, Kerala most targeted: Report*, Livemint (May. 21, 2020), https://www.livemint.com/technology/tech-news/coronavirus-related-cyberattacks-surge-by-260-during-lockdown-kerala-most-targeted-11590054440090.html.

3 Rob Schrier, *A Case for Action: Changing the Focus of National Cyber Defense*, The Cyber Defense Review, no. 2 2019, at 22, 23-28.

In addition, it provides specialist technical analysis to map out and protect the path attackers might use to breach an organisation's sensitive data and provides security strategies[4] to assure that the organisation runs its operations seamlessly without any paranoia of losing valuable assets.

Ever since World War II, warfare has dramatically changed.[5] India is continually trying to put safeguards for the same for instance the Indian armed forces have set up a specialised wing to counter Biological, Chemical and Nuclear ('BCN') warfare. BCN warfare was regarded as the warfare of the future but now with threat perceptions changing across the spectrum introduction of cyber and electronic warfare is being duly taken cognizance of. To make the defense[6] mechanism fool proof, the following efforts are worth mentioning:

- Data from the Directorate General of Commercial Intelligence and Statistics shows that power sector equipment like transmission line towers, conductors, industrial electronics, capacitors and fittings which are made in India, are still being imported. This poses a deep risk to our grid system.
- Procuring equipment from abroad including present Chinese OEMs (original equipment manufacturers) in Indian Air force Systems poses a huge risk to India's security establishment, and institutions that constitute the forefront of national security.[7]

The socio-economic infrastructure is thereby in ardent need of developing a strong cyber infrastructure that would effectively address the growing need for a cyber defensive and offensive mechanism to battle the increasing number of sophisticated malwares. The security concepts, assurances and risk management shall strive to secure and protect the cyber space. With the ever-increasing number of e-commerce activities and with the onset of the digital economy, cyber security is a growing concern for India's critical infrastructure.

Susceptibility of Financial Institutions towards Cyber Threats

Cyber threats have also emerged significantly with respect to the financial system across

4 James E McGhee, *Liberating Cyber Offense*, 4 Strategic Studies Quarterly, 46-63 45 (2016).

5 Michael Preciado, *If You Wish Cyber Peace, Prepare for Cyber War,The Need for the Federal Government to Protect Critical Infrastructure From Cyber Warfare*, 1 Journal Of Law & Cyber Warfare , 99-154, 100 (2012).

6 Martin R Stytz& Sheila B. Banks,*Toward Attaining Cyber Dominance*, 1 Strategic Studies Quarterly, 53, 55-87 (2014).

7 FJ Cilluffo&JR Clark,*Building a Conceptual Framework for Cyber's Effect on National Security*, 2 Journal Of Information Warfare, 1-16, 1 (2016).

the world especially with the advent of digital financial services such as mobile money transfers, and robust online banking systems. Some of the cyber-attacks include attacks on money transfer, ATM operations, malicious software integrated into banking systems, destruction of hardware and data of users, and disruption of internal operations.

According to an estimate by the International Monetary Fund (IMF), financial institutions could incur on an average hundred-billion-dollar losses annually due to cyber-attacks.[8] This would disrupt the financial stability across the globe, thereby eroding banks of their profits. Non-banking and other financial institutions might not only lack liquidity post such attacks rather have the potential of becoming insolvent altogether.

It is believed that cyber-attacks have the potential of leaving the targeted institution unable to operate again. In June 2018, hackers stole $530 million from Japan's Coin check cryptocurrency exchange.[9] In the absence of cyber insurance or support from the government, the exchange was left in turmoil. In 2016, the infamous malware attack on Bangladesh's Central Bank robbing it of more than $80 million brought the entire country's financial system to its knees.[10]

Financial institutions become easy targets because of their crucial role in intermediating funds. On top of it, the insurance market for cyber risk is not that significant. Most financial institutions especially in emerging economies do not carry cyber insurance. And, even if they do, the coverage is limited owing to challenges in evaluating risk because of uncertainty about cyber exposure, underestimating of risk due to lack of data, and potential contagion effects.[11]

Financial systems are also susceptible to systemic risks arising from the concentration of the Information Technology (IT) industry, whose firms use operating systems, programs, cloud servers, and electronic network hubs. Interconnected banks and transfer markets can allow shocks to spread quickly throughout the financial system. Cushioning against which is the need of the hour. While private cyber insurance[12] policies are offering data covers, they themselves can fall prey to the systemic risks. This raises a need for the public sector

8 *Estimating Cyber Risk for the Financial Sector,* IMF BLOG (Jun. 22, 2018), https://blogs.imf.org/2018/06/22/estimating-cyber-risk-for-the-financial-sector/.

9 *Japan's regulator urged Coincheck to fix flaws before $530 million cyber theft*, REUTERS (Feb. 2, 2018), https://www.reuters.com/article/uk-japan-cryptocurrency-idUSKBN1FL6PL.

10 *Malware suspected in Bangladesh bank heist,* REUTERS (Mar. 11, 2016, 10:00 AM), https://www.reuters.com/article/us-usa-fed-bangladesh-malware-idUSKCN0WD1EV.

11 Emanuel Kopp et al., *Cyber Risk, Market Failures, and Financial Stability*, IMF Working Paper WP/17/185 2017, at p. 25, 25-31.

12 Jeffrey A Franklin, 3 *CYBER INSURANCE FOR LAW FIRMS,* GPSOLO 57, 58-61 (2016).

to ensure that losses from cyber-attacks at one location do not give rise to systemic risks.

Further, the issue of regulatory arbitrage is a major reason of worry to national authorities. Financial institutions have no universal policies to regulate fintech products. While some countries have altogether banned virtual currencies, some have taken different approaches to regulate them. It is noteworthy that fintech products being digital by the very virtue cannot be contained within national borders, thereby giving rise to cyber frauds in less regulated jurisdictions. To address this lacuna, there needs to be international coordination and cooperation much to bring about clarity in the virtual space jurisdiction and safeguard the global digital products and services beforehand. Also, giving whistle-blower-like protection to employees/any other person concerned to disclose any such attack on the financial organisation is highly recommended.

Susceptibility of Organizations to various Cyber Attacks

Other organisations are equally susceptible to such attacks. A malware attack on one branch of an organization can spread rapidly through the highly interconnected IT system. This could have twofold consequences – material financial losses and diminished reputation of the organisation. Further, an organization might not disclose or publicly announce occurrence of such an attack, fearing attracting more such attacks and/or for the fear of reduced market valuation and loss of business.

Some of the valuable suggestions for the various stakeholders to counter Cyber Security Risks include undertaking thorough cyber security due diligence as part of proposed M&A transactions; due diligence in relation to key suppliers' data handing and IT security practices; cyber audit of such suppliers; Implement robust cyber security governance arrangements which should include incident response and business continuity plans; staff training on cyber security risks, especially social engineering attacks; monitoring and auditing of personnel to manage insider risks; and imported equipment should be thoroughly tested to prevent any 'trojan' or malware slipping through.

Cyber Threats to the Law Firms

Law firms being a hotspot of client information pose an attractive target for many cyber criminals as they have the capability of exposing information of not only themselves rather the numerous clients also who with faith and protection in terms of attorney-client privilege

place their valuable data[13] and information[14] with the firm.

The reason why cyber-crime pertaining to law firms is growing exponentially is because more and more companies are going virtual; that too without instituting adequate safeguards or proper training to the personnel. In May 2020, a New York-based media and entertainment law firm, Grubman Shire Meiselas & Sacks, catering to celebrity clients like Mrs. Priyanka Chopra Jonas, Lady Gaga and Nicky Minaj was cyber attacked. As per the reports[15], data including contracts, non-disclosure agreements, email addresses, phone numbers, and personal correspondences were stolen and threatened to be disclosed on public platforms.

This raises serious concerns for law firms around the world to protect their data uploaded on drives or servers especially amidst the Covid-19 crisis. One such measure adopted by the New York State Bar Association, post the cyber-attack, was to approve a recommendation by its committee on technology and the legal profession to require New York attorneys to take at least one cyber security Continuing Legal Education (CLE) credit every two years[16]. The proposal, however, still needs to be approved by the New York CLE board.

With respect to India, it is suggested that cyber security[17] courses should be incorporated in law colleges to equip future lawyers with better cyber protection knowledge and skills. Also, law firms need to invest in having a more robust IT department in order to make an online transfer of information within and outside the firm seamless and fool proof. Further, cyber law should become a mandatory subject for judiciary exams at the district level to ensure that even the civil judges are well equipped with technical know-how and can take required *suo moto* actions to ensure cyber protection in and around their areas in addition to sensitising their staff on the subject.

Cyber Defense mechanisms that can be adopted by law firms include frequent independent cyber risk audits to identify the weaker points of a server/integrated network in time; like

13 The Information Technology Act, 2000, No. 21, Acts of Parliament, Section 2(o).

14 *Id.,* Section 2(v).

15 Ashley Collman, *Hackers who stole files from a law firm to stars like Lady Gaga and Drake doubled their ransom to $42 million and threatened to release 'dirty laundry' on TrumpHackers who stole files from a law firm to stars like Lady Gaga and Drake doubled their ransom to $42 million and threatened to release 'dirty laundry' on Trump*, (May 15, 2020, 04:17 PM) https://www.businessinsider.in/international/news/hackers-who-stole-files-from-a-law-firm-to-stars-like-lady-gaga-and-drake-doubled-their-ransom-to-42-million-and-threatened-to-release-dirty-laundry-on-trump/articleshow/75757377.cms.

16 *NYSBA Eyes Mandatory Cybersecurity CLE Credit, Citing Attorneys' Heightened Cyberrisk,* New York Law Journal (June 15, 2020) https://www.law.com/newyorklawjournal/2020/06/15/nysba-eyes-mandatory-cybersecurity-cle-credit-citing-attorneys-heightened-cyberrisk/?slreturn=20200614094501.

17 *Supra* note 13, section 2(nb).

audit companies conduct audit reviews; conducting impact assessments and response plans;[18] review third-party supplier contracts to ensure that they appropriately address privacy and data protection issues, and do not transfer cyber-related risks to any organisation; manifest and review data breach response plans; lay down guidelines/specifications for third-party video conferencing applications such as Zoom, Google Meet, etc to abide by; advise clients how data protection rules of a country apply to a business and ensure compliance across the data life cycle; advise them on privacy, data protection and cyber-related legal[19] and commercial issues; build cyber risk and privacy compliance tools; get their valuable data insured; and draft guidelines for the staff to follow to rebuild from a data breach or cyber incident.

Mitigation of Risks

As cyber threats have no national boundaries, the role of international institutions becomes pertinent. International organizations like the Financial Stability Board, the Bank for International Settlements, and the International Monetary Fund can play a major part in designing internationally coordinated policies, supporting information sharing, collecting data, helping resolve cyber disputes, and containing systematic risk.

The world governments need to adopt a coordinated responsive measure to systemic cyber threats, enter into bilateral/multilateral pacts as countries do to fight terrorism, pollution, and climate change, amongst others.[20] The governmental bodies need to collect more consistent and complete data, quarterly for instance, on the frequency and impact of cyber-attacks or such attempts. This would help assess threats for the financial sector and help formulate policies on the same. It is pertinent to note that cyber threat is more of a policy matter than an IT matter on the present date. Collection of data would also incentivise reporting of breaches pertaining to privacy laws such as the European Union's General Data Protection Regulation[21], and further could be used to form a comprehensive assessment on the path and likelihood of cyber-attacks and formulate adequate policies to defend the same.

In a nutshell, assistance needs to be provided by international institutions to member

18 Chris Arney et al., *Cyber Education via Mathematical Education,* The Cyber Defense Review, no. 2 2016, at 49, 49-60.

19 Stefano Mele, *Legal Considerations on Cyber-Weapons and their Definition*, Journal Of Law & Cyber Warfare, no. 1 2014, at 52, 52-69.

20 Nir Kshetri, *Diffusion and Effects of Cyber-Crime in Developing Economies*, Third World Quarterly, no. 7 2010, at 1057, 1057-079.

21 General Data Protection Regulation, 2016, No. 679, Council of the European Parliament, (EU).

countries in order to improve their supervisory and regulatory frameworks and in setting up realistic vulnerability and recovered testing, effective supervisory practices, and contingent planning systems.[22]

It is noteworthy that while redesigning products, services and/or revamping the entire operations of an organisation might help avoid cyber risks; the possibility of new vulnerabilities coming up with the advent of new practices persists.[23]A global survey conducted by IMF with global central banks, regulatory bodies, fintech firms, and banks revealed that regulators still lacked behind in regulating the upcoming technological innovations in the fintech and tech sector and needed to ensure consumer and data protection, interoperability across users and national borders, and cyber security concerns. A shortage of coders, i.e. software developers and programmers was also observed in the survey.[24] While sandboxing facilities have been launched by various regulatory bodies around the globe, regulations for all upcoming technological developments are yet to see the light of the day.

Further, at the cost of increasing the expenses of an organization and making operations harder, security measures such as firewalls, data encryption, business continuity planning, and imparting adequate training to employees, can be considered as plausible intermediate cyber defense techniques.[25]Additionally, organizations can also transfer risks to third parties such as cyber security vendors or cyber insurance companies, but it is pertinent to mention that inadequate experience and lack of information among such third parties and overestimation of their ability to defend such risk and provide insurance cover can make these firms susceptible to financial losses and being bankrupt themselves. Also, the possibility of them becoming targets of hackers themselves cannot be ruled out.

Furthermore, national and international regulatory authorities need to provide incentives and protection from the press, to organisations, to promptly and accurately report any occurrence of cyber-attacks without fearing any loss of reputation or business.[26] Data of the same needs to be collected systematically and in a highly confidential manner in order to analyse and assess the digital footprints of attackers. Considering cyber-attacks are

22 Timothy Goines, M. *Overcoming the Cyber Weapons Paradox,* 4 STRATEGIC STUDIES QUARTERLY, 86, 86-111 (2017).

23 R Symonds, *Innovating the Prioritization of Cyber Defense*, 2 JOURNAL OF INFORMATION WARFARE, 12, 12-15 (2017).

24 Christopher Wilson et al., *Cybersecurity Risk Supervision*, INTERNATIONAL MONETARY FUND. MONETARY AND CAPITAL MARKETS (SERIES) 19/15, 7, 14-17 (2019).

25 Ball, Desmond, & Gary Waters, *Cyber Defense and Warfare*, 2 SECURITY CHALLENGES, 91, 91-98 (2013).

26 Lin, Herbert S, *Reflections on the New Department of Defense Cyber Strategy: What It Says, What It Doesn't Say*, 3 GEORGETOWN JOURNAL OF INTERNATIONAL AFFAIRS, 5, 5-13 (2016).

intrinsically criminal in nature; regulatory authorities should coordinate rapidly with law enforcement agencies of the country. Also, these regulatory authorities need to have the ability, techniques, and authority to adapt their responses as quickly as cyber threats erupt, thus need to be imparted adequate training.

Cyber Insurance

The administrative, technical and physical cyber safeguards are proactive to an attack, whereas cyber insurance is reactive to an attack. Cyber insurance is a relatively new insurance product catering to the business needs of data, to hedge risks against effects of cybercrimes such as malware, ransomware, distributed denial-of-service (DDoS) attacks, or any other method used to compromise a network and sensitive data. The threat may be internal or external. It is important to note that cyber security defense cannot be replaced with cyber insurance, as it forms an integral part of the overall cyber security machinery of an organisation. Cyber risk insurers understand the cyber security position of an organisation to issue a policy and can-do proper valuation of data. The size of the cyber insurance market is believed to be about USD 3 billion[27]. The U.S. is the biggest cyber insurance market; however, Europe and Asia are following in their footsteps due to the introduction of strict cyber and data protection regulations and amplified attacks across the world.[28]

The capabilities of the insurance industry to address novel challenges which exhibit the multi-dimensional and transnational nature of cyberspace all suggest that insurance is especially well suited to perform a pivotal role in stabilizing the domain.[29]

Determination of an engineering risk through data analysis of the insurance statistics database with respect to cyber risk coverage provided to transnational players can help determine systemic risks. Underwriters would take on the core function of assuming corporate cyber risks before providing policy coverage. A company's behavioural response to the risk environment can be influenced largely by the insurers, which supply financial incentives to deter policyholders from investment due to an increase in cyber risk in one sphere or encourage investment by extending liability coverage in a risky investment thereby assuring

27 *Cybersecurity*, National Association Of Insurance Commissioners (May 27, 2021), https://content.naic.org/cipr_topics/topic_cybersecurity.htm.

28 Michael Siegel et al., *Cyber Insurance as a Risk Mitigation Strategy,* The Geneva Association (Apr 10, 2018) https://www.genevaassociation.org/research-topics/cyber-and-innovation/cyber-insurance-risk-mitigation-strategy.

29 SA Talesh, *Data Breach, Privacy, and Cyber Insurance: How Insurance Companies Act as "Compliance Managers" for Businesses*, 43(2) Law & Social Inquiry, 417, 417-440 (2018).

the policyholder.[30] Again, the possibility of a cyber insurance firm going bankrupt cannot be overruled.

Challenges with regards to Cyber Defense

Cyber threat insurance transcends most commercial insurance lines. Unfortunately, cyber insurers do not have the underwriting experience or data analytics understanding to create underwriting arrays or data sets. This challenge not only affects insurers but re-insurers as well.[31]The Chief Information Security Officers of large corporations have reservations with respect to the insurance industry as they view insurers valuing the company based on cyber vulnerabilities[32] that exist in the system and may use that liability to provide a claim in the event of a breach that too, subject to terms and conditions. This reality makes it difficult to maintain the equilibrium of risk management and security.[33]

The cascading impact of cyber attacks greatly threatens insurance underwriters for instance if manufacturing firms rely solely on the industrial internet of things for their platform, then a cyber attack could disrupt manufacturing across an entire industry. The insurer underwriting such firms would incur massive losses from a single attack.[34]The aggregation risk of cloud computing and shared service providers amongst others are challenges that cyber security professionals face which are not yet comprehended by the insurance industry.[35]

The legacy of future technology development is based on the current cyber vulnerabilities in the environment. The cyber risk analysis market and technology market are evolving in cohorts. There are emerging start-ups focused on risk modelling and ratings that provide solutions to improve cyber insurance risk models. Examples include Bitsight, Security Scorecard, and FICO security score.[36]

30 *Id.*

31 *Id.*

32 Max Smeets, *The Strategic Promise of Offensive Cyber Operations*, 3 Strategic Studies Quarterly, 90, 90-113 (2018).

33 *Id.*

34 *Id.*

35 OECD, *Enhancing the Role of Insurance in Cyber Risk Management*, OECD Publishing (Dec. 08, 2017), http://www.oecd.org/publications/enhancing-the-role-of-insurance-in-cyber-risk-management-9789264282148-en.htm

36 Michael Siegel et al., *Cyber Insurance as a Risk Mitigation Strategy,* The Geneva Association (Apr. 10, 2018), https://www.genevaassociation.org/research-topics/cyber-and-innovation/cyber-insurance-risk-mitigation-strategy.

Modern hedging mechanisms could eventually include the monetary cost of cyber risk which will have to be shared across myriad stakeholders and different market segments. A cyber–Federal Deposit Insurance Corporation that incorporates some share of losses, especially among the most vulnerable and exposed firms, cannot only help offset costs; it can also provide cyber threat intelligence[37] sharing mechanisms.[38]

The Way Forward

The coordinated efforts of various stakeholders shall be a major breakthrough towards cyber defense. Various agencies across the borders need to work in close association and cooperation in order to curb cyber threats. Some of the major efforts and a way forward in this regard could consist of: *Firstly*, a coordinated effort at the global level to collect data in order to develop a greater understanding of the risks, nature and source of attacks and more importantly their impact on the global or domestic financial system. *Secondly*, reducing regulatory barriers, standards, terminologies, and regulations in different countries to facilitate better communication. *Thirdly*, a collaborative effort to improve the threat intelligence, resilience, responses and incident reporting to financial supervisors and law enforcement agencies seamlessly. The barrier between the private and public sectors needs to be reduced. Countries need to collaborate to share information more readily and be proactive, unlike the present pandemic where most of the responses are reactive. *Fourthly*, crisis preparation and response protocol need to be developed within regions and globally. Affected organizations should know whom to call during a crisis. *Fifthly*, averting cybercrimes by having a mandatory Know Your Customer (KYC) policy in place before opening/operating any social media account. The data of the same can be encrypted and pseudonymised for privacy concerns. *Lastly*, sensitising the general public and the youth at large about the repercussions of indulging in any such activities and apprising students and corporates of cyber ethics and the need for developing internet usage maturity should be a prime concern of policy makers across the world.

While the defense mechanism[39] is comparatively more robust in developed economies, it

37 EJ Mandt, *Integrating Cyber-Intelligence Analysis and Active Cyber-Defense Operations,* 1 Journal Of Information Warfare, 31, 31-48 (2017).

38 D. Disparte, *A Cyber Federal Deposit Insurance Corporation?: Achieving Enhanced National Security*, *7*(2) PRISM, 52, 52-65 (2017).

39 SL Russell & SC Jackson, *Operating in the Dark: Cyber Decision-Making from First Principles*, 1 Journal Of Information Warfare, 1, 1-15 (2018).

is the emerging economies that are gradually switching to online mode of operations[40] that need international attention and collaboration immediately in order to make a more secure and seamless digital ecosystem.[41]

Conclusion

It is imperative to note that the pace at which the business houses, companies, law firms, and educational institutions have started operating in the virtual space, any virus that hits the machines in the near or far future has the potential to disrupt all data and bring the whole world economy to a standstill.

With information, no longer confidential and safe, it possesses the risk to overthrow the ruling parties across the world by disclosing their shady deals, can make the stock market take a dip, make law firms lose cases and their clients eventually by revealing the truth behind the matter, and leak all the examination papers and entrance tests that are saved in the virtual space to assess the intelligence of students. Repercussions can be far worse than what can be anticipated.

Thus, cyber frauds, threats, attacks are largely known to impact the national security, social well-being and economic fabric of the country pointing towards the ever-growing demand for a secure cyber environment to protect the citizens in real time. Therefore, it is essentially ardent to have employees and staff with basic cyber security[42] skills along with adequate budgets for advanced infrastructure, training and resources to develop required skills. An effective cyber surveillance system can only come into existence with requisite skill development, which consequently provides for a secure action plan in case the need to combat cyber-attacks arises.

40 C Maathuis et al., *Developing a Cyber Operations Computational Ontology*, 3 Journal Of Information Warfare, 32, 32-49 (2018).

41 Michael Sulmeyer,*Campaign Planning with Cyber Operations,* 3 Georgetown Journal Of International Affairs, 131, 131-37 (2017).

42 Sitara Noor, *Cyber (In) Security: A Challenge to Reckon With,* 2(3) Strategic Studies, 1, 1-19 (2014).